IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

UNITED STATES OF AMERICA, v. **MICHAEL HARMON**, Defendant.	Case No. 3:18-cr-221-SI **OPINION AND ORDER**

Billy J. Williams, United States Attorney, and Ravi Sinha, Assistant United States Attorney, UNITED STATES ATTORNEY'S OFFICE FOR THE DISTRICT OF OREGON, 1000 SW Third Ave., Suite 600, Portland, OR 97204. Of Attorneys for the United States of America.

Matthew A. Schindler, 501 Fourth Street, Suite 324, Lake Oswego, OR 97034. Of Attorney for Defendant Michael Harmon.

Michael H. Simon, District Judge.

On March 30, 2018, federal law enforcement officers obtained three laptop computers from Defendant Michael Harmon based on Defendant's verbal and written consent to search those computers for child pornography. Defendant told the officers that the laptop computers contained deleted-but-recoverable images of child pornography, and the officers took the computers to the FBI's Regional Computer Forensics Laboratory to conduct the search. On April 9, 2018, Defendant revoked his consent to search, and the FBI halted its examination of the

computers. After federal law enforcement officers obtained a search warrant, the examination resumed on Monday, April 16, 2018. The FBI has not yet returned the computers to Defendant. Defendant has moved to suppress all evidence seized from the computers, arguing that the government has taken "too long" to search the computers and that the computers have not yet been returned to him. For the reasons that follow, Defendant's motion to suppress is DENIED.

STANDARDS

The Fourth Amendment provides for "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend. IV. It also provides that "no Warrants shall issue" without probable cause. *Id.* A judge may issue a search warrant if "there is a fair probability that contraband or evidence will be found in a particular place." *United States v. Underwood*, 725 F.3d 1076, 1081 (9th Cir. 2013) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). When a search has taken place in violation of the Fourth Amendment, the exclusionary rule may require that the evidence obtained as a result of the search be suppressed. *See Davis v. United States*, 564 U.S. 229, 236 (2011).

Searches and seizures of electronic records and personal computers "pose unique challenges for 'striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures.'" *United States v. Schesso*, 730 F.3d 1040, 1042 (9th Cir. 2013) (quoting *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam)). Personal electronic devices, like laptops, often "contain vast quantities of intermingled information, raising the risks inherent in over-seizing data." *Id.* As technology changes and evolves, courts have sought to provide clarity on striking the right balance between individual privacy and law enforcement. For these reasons, "law enforcement and judicial officers must be especially cognizant of privacy risks when drafting and executing search warrants for electronic evidence." *Id.* The Ninth Circuit

does not require that warrants for digital storage media specify a particular search protocol, *see United States v. Hill*, 459 F.3d 966, 978 (9th Cir. 2006), but law enforcement officers are "always limited by the longstanding principle that a duly issued warrant . . . may not be used to engage in a general, exploratory search," *id.* (internal quotations omitted).

DISCUSSION

Defendant does not challenge the validity of the search warrant or argue that it was unlawfully obtained. Instead, he argues only that the FBI has taken too long to search his laptop computers. He adds that the government has gone past the deadlines for review set forth in the warrant and that this failure to comply with the terms of the warrant has violated his Fourth Amendment rights and has caused him prejudice. According to Defendant, his personal computers that were seized contain vast amounts of private, personal, and privileged information in addition to the material that was the subject of the search warrant. Defendant argues that this presents a danger that any search of his computers may become a search under an overbroad general warrant. The remedy he seeks for this prejudice is suppression of all evidence contained on his three laptop computers and the prompt return of his computers.

In the search warrant, the government stated that it would perform the initial examination of the computers within 120 days from the date of execution of the warrant and complete its review within 180 days. If the examination revealed that the devices contained no data falling within the ambit of the warrant, the government promised to return the computers to Defendant. Law enforcement, however, would continue to examine any files or data falling within the purview of the warrant that the search uncovered. Files or file folders that contained no data falling within the scope of the warrant would not be searched without express authorization from the Court. Finally, the warrant stated that the government may retain the devices as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings

against the computers and the data they contain. The FBI completed its initial examination of two of the three computers in late April 2018. According to the government, the two laptop computers that the FBI examined contained images and videos of suspected child pornography. The third laptop is encrypted, and the FBI has not yet been able to access it.[1]

Based on Defendant's own statements that the laptop computers contained child pornography, officials had probable cause to search the contents of all three laptop computers for child pornography, and they lawfully obtained a warrant to do so. Offsite examination of the laptop computers was necessary because the files on the computers had, in some cases, been erased or encrypted, requiring more time and expertise to access them. *See Comprehensive Drug Testing, Inc.*, 621 F.3d at 1168. The files, therefore, could not have been quickly reviewed and required prolonged offsite analysis. *See, e.g. United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982).

One of the unique problems posed when searching digital files, as opposed to paper files, is that it is often difficult "to be sure exactly what an electronic file contains without somehow examining its contents—either by opening and looking, using specialized forensic software, keyword searching or some other such technique." *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1176. "Over-seizing" is therefore "an inherent part of the electronic search process," as FBI officers must sort through thousands or hundreds of thousands of files while searching for the suspected contraband. *Id.* at 1177. The Ninth Circuit has upheld broad searches of a defendant's personal electronic devices, *see United States v. Hay*, 231 F.3d 630, 636-37 (9th Cir. 2000), and prevailing law in the Ninth Circuit does not mandate that the warrant include a search protocol to

[1] Defendant's repeated assertion that searching a computer is "something that could be done in 24 hours" is inaccurate, especially when a computer has been locked and encrypted, and is not consistent with the realities of the time it takes to break encryption and recover hidden or deleted files.

govern the examination of electronic storage media. *See Schesso*, 730 F.3d at 1049; *Hill*, 459 F.3d at 978.

The exclusionary rule does not warrant suppression of the evidence uncovered on Defendant's laptop devices. Even though the review of the third laptop computer was not completed within the deadlines outlined in the warrant, Defendant cannot establish any unreasonable prejudice resulting from the FBI's alleged failure to comply with the search deadlines stated in the warrant. *See id.* It is Defendant's own encryption that has thus far prevented the FBI from more timely searching the third laptop, and there has been no unreasonable delay on the part of the FBI. *Cf. United States v. Sullivan*, 797 F.3d 623, 634-35 (9th Cir. 2015) (holding that government had reasonable basis for delay when assistance from another agency was required). The FBI completed its review of two of the computers within the timeframe outlined in the warrant and has made the contents of those computers available to Defendant for his review. Consistent with the warrant, because the FBI located suspected contraband on the computers, it could continue examining the files or data recovered and retain the computers as instrumentalities of a crime. The government's interest in retaining the computers is compelling. *See id.* at 634.

Further, even if the warrant were in some way deficient, Defendant has provided no evidence to suggest that the FBI's reliance on the warrant was not objectively reasonable and that the good faith exception to the exclusionary rule should not apply. *See United States v. Leon*, 468 U.S. 897, 922 (1984). When an officer conducts a search in good faith reliance upon a facially valid warrant, suppression is not warranted unless the officer's reliance on the warrant was not "objectively reasonable," the magistrate judge "wholly abandoned his judicial role," or the officer acted in bad faith by misleading the magistrate judge. *Id.* at 922-23. Defendant does

not argue that any of these things has occurred; nor does it appear from the record that there is any basis to argue that it was not reasonable for the FBI to continue to attempt to access the third computer or to continue to review the files obtained from the other two computers.

When a defendant's Fourth Amendment rights have been violated, the evidence generally must be suppressed, *see, e.g.*, *Mapp v. Ohio*, 367 U.S. 643, 648 (1961), but the Fourth Amendment does not mandate the return of seized property. Defendant argues that, to ensure compliance with the Fourth Amendment, the laptop computers must be returned to him pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure. Although a motion made under Rule 41(g) should be presumptively granted if the government "no longer needs the property for evidence," that is not the case here. *United States v. Fitzen*, 80 F.3d 387, 388 (9th Cir. 1996). This presumption can be rebutted if the government's continued retention of the seized property is "reasonable under all of the circumstances" *United States v. Kriesel*, 720 F.3d 1137, 1145 (9th Cir. 2013) (quoting *Ramsden v. United States*, 2 F.3d 332, 336 (9th Cir. 1993)).

Two of the devices that Defendant seeks to have returned have been examined and credibly found to contain child pornography, which Defendant may not lawfully possess. The government has a legitimate interest in retaining the third laptop because the government continues to attempt to defeat Defendant's encryption of that device. Because the computers are reasonably believed to contain contraband, they likely will be needed for evidence at trial. In addition, federal law requires that "any property or material that constitutes child pornography shall remain in the care, custody, and control of either the Government or the court." 18 U.S.C. § 3509(m). The continued retention of the seized property, therefore, is reasonable. *See Kriesel*, 720 F.3d at 1137.

Further, Defendant has not suffered unfair prejudice from not having possession of his computers. The conditions of Defendant's release prohibit him from directly or indirectly using or possessing "a computer or electronic media, including any devices and cellular phones, with internet access capabilities or access[ing] a computer or electronic media, without prior approval of Pretrial Services." When individuals cannot make use of the seized property, "their possessory interest in that property is reduced." *Sullivan*, 797 F.3d at 633. Defendant argues that small-business-owners or individuals who require access to medical records kept on their computer might be prejudiced by the government's continued retention of a computer, but he does not argue that he has been unfairly prejudiced in those ways.

Defendant also argues that he has been prejudiced by the government's decision to retain the laptop computers because it impedes his ability to review the evidence against him. That might be a serious and unfair prejudice but for the fact that the government asserts that it has made the evidence seized from the laptop computers available to Defendant and Defendant's counsel for review. The government, therefore, is authorized to retain the devices, and the evidence obtained from the searches of the devices will not be suppressed.

CONCLUSION

Defendant's motion to suppress (ECF 25) is DENIED.

IT IS SO ORDERED.

DATED this 5th day of November, 2018.

/s/ *Michael H. Simon*
Michael H. Simon
United States District Judge